Exelon Generation
4300 Winfield Road
Warrenville, IL 60555

www.exeloncorp.com

Exelon Nuclear

10 CFR 50.90

RS-08-119
September 12, 2008

U. S. Nuclear Regulatory Commission
ATTN: Document Control Desk
Washington, DC 20555-0001

LaSalle County Station, Units 1 and 2
Facility Operating License Nos. NPF-11 and NPF-18
NRC Docket Nos. 50-373 and 50-374

Subject: Supplemental Information Concerning License Amendment to Allow Ganged Rod Drive Capability of the Rod Control Management System

References:

1. Letter from D. M. Benyak (Exelon Generation Company, LLC) to U. S. NRC, "Request for License Amendment to Allow Ganged Rod Drive Capability of the Rod Control Management System," dated August 14, 2007

2. Letter from S. P. Sands (U. S. NRC) to C. G. Pardee, (Exelon Generation Company, LLC), "LaSalle County Station, Units 1 and 2 - Request for Additional Information Related to Request for License Amendment to Allow Ganged Rod Drive Capability of the Rod Control Management System (TAC Nos. MD7900 and MD7901)," dated August 1, 2008

3. Letter from P. R. Simpson (Exelon Generation Company, LLC) to U. S. NRC, "Supplemental Information Concerning License Amendment to Allow Ganged Rod Drive Capability of the Rod Control Management System," dated September 2, 2008

In Reference 1, Exelon Generation Company, LLC (EGC) requested an amendment to Facility Operating License Nos. NPF-11 and NPF-18 for LaSalle County Station (LSCS), Units 1 and 2. The proposed change revises the LSCS licensing basis to allow ganged rod drive capability of the Rod Control Management System.

This letter provides supplemental information to the NRC in response to requests for additional information (RAIs) that were provided to EGC in Reference 2, and clarified during teleconferences between EGC and the NRC on June 19, June 26, July 10, and July 21, 2008. The attachment and enclosure to this letter, in concert with a partial response submitted in Reference 3, completes EGC's response to the Reference 2 RAIs.

The information provided in this letter does not affect the No Significant Hazards Consideration, or the Environmental Consideration provided in Attachment 1 of the original license amendment request as described in Reference 1.

In accordance with 10 CFR 50.91(b), "State consultation," EGC is providing the State of Illinois with a copy of this letter and its attachment to the designated State Official.

There are no regulatory commitments contained in this letter.

If you have any questions concerning this letter, please contact Mr. John L. Schrage at (630) 657-2821.

I declare under penalty of perjury that the foregoing is true and correct. Executed on the 12th day of September 2008.

Respectfully,

Patrick R. Simpson

Patrick R. Simpson
Manager - Licensing

Attachment: Supplemental Information Concerning License Amendment to Allow Ganged Rod Drive Capability of the Rod Control Management System

Enclosure: Summary of System Functional Level Common-mode Software Failures

Background

In a letter dated August 1, 2008 (i.e., Reference 2), the NRC transmitted Requests for Additional Information (RAIs) to Exelon Generation Company, LLC (EGC) concerning a license amendment request (LAR) for LaSalle County Station (LSCS) that was submitted in Reference 1. EGC provided a partial response to the RAIs in Reference 3. The information below provides a final response to the remaining RAIs (i.e., EICB-1, EICB-3, EICB-5, EICB-6, and EICB-7). EGC has discussed this response schedule with the NRC (i.e., Mr. Stephen P. Sands, the NRR Project Manager for LSCS).

<u>NRC Request EICB-1</u>

Section 1.2, 1st Paragraph: *"EGC is replacing the original Rod Worth Minimizer (RWM) and the Reactor Manual Control System (RMCS), which is comprised of the Rod Drive Control System (RDCS) and the Rod Position Indication System (RPIS) with a new Rod Control Management System (RCMS). The current RMCS uses discrete digital electronics and dynamic logic to control rod motion. The replacement RCMS system will be a digital microprocessor-based system. The new system will also incorporate the RWM within the system, eliminating the need for a separate RWM computer."*

The original design feature included separate computer for the RWM function, however, the proposed design incorporates the RWM and all the subsystems of the RMCS in a single microprocessor based system. Please summarize the failure modes that have been evaluated for the new system, and describe the consequences that result from these failures. This description should include the elements that will be employed to demonstrate that the potential vulnerabilities associated with common-mode software failures have been adequately addressed and justification that these consequences will not put the plant into a new and unanalyzed state.

EGC Response

In the Reference 1 LAR, EGC described the process that was used for the design, development, validation, and testing of the Rod Control Management System (RCMS) software (i.e., the GE NUMAC process). While the implementation of this process during the design and development of the RCMS helps minimize the potential for a common-mode software failure, it cannot eliminate the potential for a theoretical failure simultaneously affecting multiple RCMS components. Nor can the implementation of the process provide a quantifiable probability for the occurrence of a theoretical common-mode software failure (i.e., resulting in an uncontrolled rod gang withdrawal).

However, the combination of several elements associated with the design and operation of the RCMS system, when viewed as a multi-layer defense system, provide reasonable assurance that potential vulnerabilities to a theoretical common-mode software failure have been adequately addressed. EGC has concluded that the combination of: 1) a rigorous NUMAC software development and testing process; 2) the RCMS system design process, which included a Failure Modes and Effects Analysis (FMEA); 3) inherent RCMS design features; 4) the expected operator actions, in accordance with site approved training and procedures; and 5) the safety-related neutron monitoring and reactor protection systems, taken as a whole, provide the necessary level of assurance that the vulnerabilities to a theoretical common-mode software failure have been adequately addressed.

The first three layers of this the multi-layered defense system are described below. The fourth layer has been described in the response to EICB-2 in Reference 3, the response to NRC Request 3 in Reference 4, and in section 4.0 of Reference 5. The fifth layer of defense is described in the LSCS Updated Final Safety Analysis Report (UFSAR), Section 7.2, "Reactor Protection System," and Section 7.6.3, "Neutron Monitoring System Instrumentation and Controls."

In addition, EGC has verified that, in the event of an uncontrolled rod gang withdrawal due to a common-mode software failure, despite the multi-layered defense system, the potential consequences will be bounded by the consequences of a previously analyzed accident. This verification was described in the response to RAI SRXB-5 in Reference 3.

Finally, EGC has summarized the theoretical common-mode software failures that could impact each functional area of the RCMS. This summary is provided in the Enclosure. For each common-mode software failure, including the theoretical inadvertent ganged-rod withdrawal error, EGC has identified the consequences, the method of identification, and the bounding end state. As described in the Enclosure, the bounding end states would not put the plant in a new or unanalyzed state.

Defense Layer 1 - Rigor of NUMAC Software Development Process

The RCMS software, although not safety-related, was developed using the General Electric Hitachi (GEH) NUMAC Software Configuration Management Plan (SCMP), the NUMAC Software Management Plan (SMP), and the NUMAC Software Verification and Validation (V&V) Plan (SVVP) process, as modified in GEH Nuclear Energy DRF 0000-0038-3006, Revision 2, "Rod Control Management System (RCMS) Software Development Plan," dated March 9, 2007, which was provided in Attachment 1 of Reference 1 (i.e., item 1). In addition, EGC provided, in Attachment 2 of Reference 1, the RCMS-specific NUMAC software management plan and NUMAC software verification and validation plan (i.e., items 2 and 3). The RCMS Software Development Plan specifically addresses issues such as design control, change control, documentation, record keeping, independent verification, and software development requirements, as described in RG 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants."

Although the application of the NUMAC process to the RCMS is not safety-related, GEH utilized the standard safety-related software development process and standard GEH procedures (i.e., applicable for both safety-related and non-safety-related applications).

The RCMS is a member of GE's Nuclear Measurement Analysis and Control (NUMAC) product line. This "family" of microprocessor-based instruments and systems has a proven record of reliability, with over 20 years of product operating experience with over 3700 unit-years on-line. Over 700 NUMAC units have been installed in 54 BWRs worldwide

During the RCMS design and development, GEH conducted several independent internal reviews by GEH Chief Engineers to validate that the NUMAC processes were correctly implemented for the RCMS software. These RCMS design reviews concluded that sufficient reviews and testing was done to ensure product quality.

GEH also implemented a comprehensive V&V testing program for the LSCS RCMS software, where all requirements were tested using a traceability matrix. This V&V program demonstrated that all requirements were tested, either through black-box or white-box testing. The V&V testing was designed and performed by independent teams at GEH. EGC also independently implemented the V&V procedures on the LSCS Unit 1 RCMS equipment at LSCS, and obtained similar results.

Defense Layer 2 - RCMS system design process

The RCMS components have been designed and built to the GE Nuclear Energy Quality Assurance Program (i.e., NEDO-11209 04A, Revision 8, dated March 31, 1989), which has been reviewed and accepted by the NRC. This program meets the requirements of ANSI N45.2, and 10 CFR 50, Appendix B.

As part of the RCMS design process, GEH and EGC developed an FMEA that evaluated approximately 200 different failure modes, including ganged rod withdrawal failure modes. EGC provided the FMEA in Attachment 2 of Reference 6. The FMEA identifies, for each RCMS component (e.g., RCMS Controller, File Control Processor, etc.) and function (e.g., internal and external communication, signal evaluation, output signal control, etc.), the failure mode, the cause, the method of detection, the inherent compensating provision, and the effect upon the system. The analyzed causes for the various failure modes include internal logic errors and computer fault/internal processing errors.

FMEA items 110, 111, and 112 (i.e., sheets 49 and 50 in Attachment 2 of Reference 6) address failure modes and inherent compensating provisions specific to the ganged-rod drive capability of the RCMS Controller. However, the causes that are specified for failure modes of other components and functions also include internal logic errors and computer fault/internal processing errors. The inherent compensating provisions for these other components, functions, and failure modes are also applicable to ganged-rod drive capability.

Defense Layer 3 - RCMS design features

Although the RCMS system is not safety-related, it utilizes redundant hardware and software for high reliability, with internal comparison and self-test functions. Within the RCMS, software redundancy and diversity is provided by the use of different types of operating systems for the different component types (i.e., RCMS Controllers, MCR Controllers, Interface Units, and File Control Processors), different software installation methods, different running tasks, different input variables, and different output signals. The redundant hardware and software also incorporate a cross-compare function that requires complete agreement in signals between the diverse components in order for a rod gang to operate. Taken as a whole, the hardware and software diversity and redundancy further reduces the susceptibility of the RCMS to a common-mode software failures.

a) Software and Hardware

The RCMS utilizes three diverse types of NUMAC processors and operating systems (OSs):

- The Interface Units use a standard NUMAC chassis including the proven NUMAC NM-386 operating system.
- The Controllers use RTOS-32, which has been used for previous non-safety applications in the Advanced Boiling Water Reactor.
- The File Control Processors (FCPs) use a simple 5 millisecond execution loop to obtain and process control rod position information from the probe multiplexer cards.

The RCMS and MCR Controller software is pre-installed on separate compact flashes for each controller. These flash cards contain the configuration files that establish each application that the specific controller performs. Although the application software is the same for the RCMS and MCR Controllers, there are controller-specific (i.e., RCMS and MCR) sampling and control functions. Thus, the running software tasks at any instant are different. For example, RCMS Controllers provide rod control permissives/logic while the MCR Controllers primarily provide the operator graphical user interface functions.

The software for the RCMS and MCR Interface Units is pre-installed on EPROMs. Although the EPROMs for the RCMS and MCR Interface Units are the same, the tasks and logic are different. The RCMS Interface Units provide plant inputs/outputs and transponder control, while the MCR Interface Units provide operator inputs and RBM outputs.

FCPs acquire rod positions, and RCMS Controllers decode that position data. RCMS Interface Units acquire plant-level and bypass signals, and RCMS Controllers process the data. MCR Interface Units acquire operator requests and MCR Controllers send this to the RCMS Controllers for further action and voting. This communication and control protocol provides an additional level of software separation and added redundancy.

b) Cross-Compare Validation and Self-Test

If rod motion, requested by the MCR Controller, is allowed by the various inputs to the RCMS Controller (e.g., Rod Block Monitor, Nuclear Instrumentation, etc.) and by the programmed rod sequence, the RCMS Controller will initiate commands to its associated RCMS Interface Unit. The RCMS Controllers will perform a cross-compare function that compares input and output signals to and from the two RCMS Controllers to confirm that each controller produces the same output signal when supplied with the same input signal. A cross-compare disagreement causes a rod block. This cross-compare function is a barrier to ensure proper controller performance. In addition to the cross-compare function, the RCMS Controllers are designed with self-test diagnostics that will provide an alarm, and potentially rod blocks, upon recognition of malfunctions.

The RCMS Interface Units provide the internal and external system input and output between the RCMS Controllers and other plant systems, and to the Branch Junction Modules and hydraulic control unit (HCU) Transponders. Each RCMS Interface Unit communicates with both RCMS Controllers. Similar to the RCMS Controllers, each of the RCMS Interface Units include a microprocessor that packages and processes data sent to, or received from, the RCMS

Controllers; performs cross-comparisons of the data from the two controllers; and performs local self-test diagnostics.

During operation, multiplexed rod movement command outputs from the RCMS Controllers to the HCU Transponders are generated independently in each controller and compared independently in each RCMS Interface Unit. If a disagreement is detected in either RCMS Interface Unit, the signal is not sent to the transponders. If both RCMS Interface Units find the command signals to be in agreement, the commands will be transmitted to the transponders, the responses will be received and compared, and the signals will be transmitted to the RCMS Controllers, which will also perform a cross-comparison of the signals.

The MCR Controllers communicate with the RCMS Controllers, the MCR Interface Units, and either the Rod Select Module or the Core Map Display Module. The MCR Controllers are designed with self-test diagnostics that will provide an alarm to the operator upon recognition of malfunctions. The MCR Controllers have two functions. One function is a single channel display/touch screen interface with separate independent displays. The second is a dual-channel redundant operator interface/comparison function.

The processing of signals for rod movement requests by the MCR Controllers is a redundant function in that if the command request from either of the two MCR Controllers sent to both RCMS Controllers is not in agreement, no action will be taken by the logic in the RCMS Controllers. Both MCR Controllers receive the selected rod and rod driving information from both RCMS Controllers. If either MCR Controller finds either the rod selection or rod driving signals from the two RCMS Controllers to be in disagreement, an alarm is provided on the MCR Controller's associated display. If rod selection is not in agreement, rod selection confirmation is not provided to the MCR Controller's associated display, and a no-rod-selected signal is sent to the associated RBM channel.

NRC Request EICB-3

Section 3.2.2 - Comparison of New RCMS to Existing RMCS: The last paragraph on page 10 of 49 states that, *"The use of the flat-panel touch screen displays instead of the discrete indicators creates a fundamental change to the human system interface." The last paragraph of this section states, "As is the case with the existing RMCS and RWM, the components for the replacement RCMS are not safety-related or seismic, but are seismically installed in the cabinets and panels to satisfy seismic II/I concerns, where required."* The touch-screen VDU is not seismically qualified and is, therefore, subject to multiple spurious actuations in case of a seismic event. Please explain why such an event could not place the plant in a new unanalyzed condition.

EGC Response

The RCMS utilizes the same operating scheme for rod motion pushbuttons as currently installed for the Reactor Manual Control System. The RCMS pushbuttons are mechanically recessed into the Rod Select Console requiring depression slightly below the surface of the console, similar to the surrounding collar of the original design. In addition, as with the current rod control design, continuous rod withdrawal with RCMS requires the simultaneous pressing of the two pushbuttons on opposite sides of the Rod Select Console (i.e., requiring two-handed operation). These pushbuttons are independent of the touch-screen. Thus, inadvertent movement of a control rod or gang cannot result solely from multiple spurious actuation of the rod select VDU.

NRC Request EICB-5

Section 3.3.4: The second paragraph states, *"From a software perspective, the NUMAC process that was used for development and validation of the RCMS software, as described in Section 3.2.7 above, yields software that has a low probability of failure. However, any software-based system can generate random faults. Based on the development and validation process, there is a very low probability of a common mode failure in those areas that are tested in the V&V testing process. Because of this low probability of a common mode failure, random errors are assumed in only one program of one component."*

Given the NRC concern that software design errors are a credible source of common-mode failures (i.e., as discussed in Branch Technical Position HICB-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems"), please justify or revise the statement regarding the low probability of failure, consistent with the guidance in HICB-19. In addition, identify the key defense-in-depth and diversity elements that will be employed to demonstrate that the potential vulnerabilities associated with common-mode software failures have been adequately addressed.

EGC Response

In the Reference 1 LAR, EGC described the process that was used for the design, development, validation, and testing of the RCMS software (i.e., the GE NUMAC process). While the implementation of this process during the design and development of the RCMS helps minimize the potential for a common-mode software failure, it cannot eliminate the potential for a theoretical failure simultaneously affecting multiple RCMS components. Nor can the implementation of the process provide a quantifiable probability for the occurrence of a theoretical common-mode software failure (i.e., resulting in an uncontrolled rod gang withdrawal).

However, the combination of several key elements associated with the design and operation of the RCMS system, when viewed as a multi-layer defense system, provide reasonable assurance that potential vulnerabilities to a theoretical common-mode software failure have been adequately addressed. Specifically, the combination of 1) a rigorous NUMAC software development and testing process; 2) the RCMS system design process, which included a Failure Modes and Effects Analysis (FMEA); 3) inherent RCMS design features; 4) the expected operator actions (in accordance with site approved training and procedures); and 5) the safety-related neutron monitoring and reactor protection systems, taken as a whole, provide the necessary level of assurance that the vulnerabilities to a theoretical common-mode software failure have been adequately addressed. Additional detail regarding these key elements is provided in the response to EICB-1.

NRC Request EICB-6

The licensee has stated that the new RCMS pushbuttons are slightly smaller than the current pushbuttons, providing a smaller target for a seismic event. Please provide justification for the conclusion that these smaller switches have similar or better seismic withstand capability as compared with the existing switches. Compare mechanical rigidity and spring strength and any other pertinent design characteristics to back up the justification.

The licensee has stated that *"In the event of a seismic event, these displays are adequately mounted to the H13-P603 panel and are not sensitive to falling objects or debris from other systems."* Please confirm that all the equipment in the vicinity and above the VDU touch-screen is mounted seismically to protect the VDUs from falling debris and causing spurious selection of rods for movement.

EGC Response

The VDU touch-screens are mounted in the center of the H13-P603 panel. The H13-P603 panel is classified as non-safety related but seismically mounted. Located above the VDU touch-screens is the top portion of the H13-P603 panel, the MCR ceiling, and lights. The RCMS components in the top portion of the H13-P603 panel, as well as all other components are seismically installed in the panel to satisfy Seismic II/I concerns. The MCR ceiling and lights are designed and installed to meet Seismic Category I requirements. Therefore, all the equipment in the vicinity and above the VDU touch-screen is mounted seismically to protect the VDUs from falling debris and causing spurious selection of rods for movement.

In addition, the VDU screens are capacitive touch. Selection of items on the screen occurs when an object with the capacitance of a human finger touches the screen. Other objects such as pens and notebooks have no affect and cannot be used to select items on the screen. This provides additional verification the VDUs are protected from falling debris that would cause spurious selection of rods for movement.

Also, see the response to NRC Request EICB-3.

NRC Request EICB-7

Following two-way messages provide communication between Level 4 and Level 3 equipment:

- Messages sent to RCMS Controller by the PPC Over the Data Connection
- Messages sent to RCMS Controller by the PPC Over the Status Connection
- Messages sent to RCMS Controller by the RWM Sequence Computer

Please confirm that all the communication data is predefined and any data which is not predefined will be ignored by the receiving system. How is unrecognized data handled within the receiving system? Does every message have the same message field structure and sequence, including message identification, status information, data bits etc. in the same location in every message. Every datum should be included in every transmit cycle, whether it has changed since the previous transmission or not, to ensure deterministic system behavior.

Appendix B, Section 5, Monitoring of boundary interfaces provides guidance on setting up the boundary interfaces with security components such as firewalls, network intrusion detection system, host intrusion detector systems etc. Please describe your boundary interfaces and their compliance with NEI 04-04.

Appendix B, Section 7, Variations on the model provides further guidance for deviations from the 4 layer model. Since LaSalle is deviating from this model, please describe how LaSalle meets the guidance of this section of NEI 04-04 [Nuclear Energy Institute].

EGC Response

Communication Data

All RCMS communications data is pre-defined as described in Reference 1, Attachment 2, Item 6, GE Nuclear Energy Specification 26A6517, Revision 3, "Rod Control Management System (RCMS) External Interface Specification," and Item 9, GE Nuclear Energy Specification 26A6582, Revision 2, "Rod Control Management System (RCMS) Internal Communication Protocol Specification."

When a message is received by RCMS, it is first validated for checksum integrity.

1. If the checksum is not valid, the message is discarded and an event message, similar to the following is logged: "MON: CHECKSUM ERROR Message NN from MCR." In addition, a checksum error count is also maintained by communications link that could be examined on COMM STATUS screen.

2. If the checksum is valid, but it is an unrecognized message, the message is discarded and an event message similar to the is logged: "MON: Unhandled MCR Message MsgID NN."

3. If the checksum is valid and it is a recognized message, the message is then validated for content integrity. If content integrity is not satisfied, this message is discarded and an alarm message similar to the following is logged: "Failed Validation: Parameter Change Request Message."

With respect to message field structure and sequence for communication between the RCMS Controllers and the PPC and RWM, including message identification, status information, data bits etc., the "Rod Control Management System (RCMS) External Interface Specification (i.e., Reference 1, Attachment 2, Item 6) describes the following information:

- Section 3 provides a table that describes the structure of messages exchanged between RCMS Controller and the PPC, as well as sub-systems internal to RCMS. In addition, Section 3 describes the Checksum Algorithm and byte ordering.
- Section 4 defines the source and destination IDs.
- Section 7 provides detailed message descriptions between the RCMS Controller and both the PPC and RWM, over both the data connection and status connection. This includes message format (i.e., offset, size, label and contents).
- Section 8 provides a bit by bit description of all messages.

Message field structure and sequence for internal communication between all RCMS components is described in the "Rod Control Management System (RCMS) Internal Communication Protocol Specification," (i.e., Reference 1, Attachment 2, Item 6). This document defines internal interfaces of the microprocessor-based RCMS, in the same manner as the external interface specification.

NEI 04-04, Appendix B

Section 3.2.5 of Reference 1 states that all RCMS components, with the exception of the RCMS Controllers, are connected to each other via a dedicated private network, with no direct connection to the higher level networks. Each RCMS Controller is connected to both the Plant Process Computer (PPC) and the RWM Sequence Computer via dedicated connections. These connections only provide bi-directional messaging capabilities between the RCMS Controllers and both the PPC and RWM systems; no access to RCMS control functions is directly available via these links. The boundary interface between the RCMS Controllers and both the PPC and RWM is a Nokia IP530 appliance running Checkpoint Version 5.4 software firewall. EGC has determined that the bi-directional messaging capability is an acceptable variation from the Defensive Model depicted in Figure 6.1 of NEI 04-04.

The LSCS configuration conforms to the Modified 4-layer Model depicted in Appendix B, Section 7, Figure B-5, of NEI 04-04, in that the bi-direction communication capability is messaging only. The RCMS control communication capability is unidirectional. Defensive Level 3 is effectively provided by the robust firewall, in concert with the characteristics of the data being transferred between the RCMS Controller and the PPC or the RWM sequence computer, as described above and in Attachment 2 of Reference 1, Item 9.

References:

1. Letter from D. M. Benyak (Exelon Generation Company, LLC) to U. S. NRC, "Request for License Amendment to Allow Ganged Rod Drive Capability of the Rod Control Management System," dated August 14, 2007

2. Letter from S. P. Sands (U. S. NRC) to C. G. Pardee, (Exelon Generation Company, LLC), "LaSalle County Station, Units 1 and 2 - Request for Additional Information Related to Request for License Amendment to Allow Ganged Rod Drive Capability of the Rod Control Management System (TAC Nos. MD7900 and MD7901)," dated August 1, 2008

3. Letter from P. R. Simpson (Exelon Generation Company, LLC) to U. S. NRC, "Supplemental Information Concerning License Amendment to Allow Ganged Rod Drive Capability of the Rod Control Management System," dated September 2, 2008

4. Letter from P. R. Simpson to U. S. NRC, "Supplemental Information Concerning License Amendment to Allow Ganged Rod Drive Capability of the Rod Control Management System," dated May 13, 2008

5. Letter from J. A. Bauer (Exelon Generation Company, LLC) to U. S. NRC, "Supplemental Information Concerning License Amendment Request to Revise License Basis to Allow

Ganged Rod Drive Capability of the Rod Control Management System (RCMS)," dated June 1, 2006

6. Letter from J. A. Bauer (Exelon Generation Company, LLC) to U. S. NRC, "Supplemental Information Concerning License Amendment Request to Revise License Basis to Allow Ganged Rod Drive Capability of the Rod Control Management System (RCMS)," dated May 10, 2006

The following table summarizes an evaluation of the system functional level common-mode software failures, the resulting consequences for each, manner of identification, and the bounding end state. The final evaluated failure is the theoretical inadvertent ganged rod withdrawal error at low power and high power conditions. All preceding failures assume a common-mode software failure without the inadvertent ganged rod withdrawal error (i.e., a common-mode failure occurs but is not self-revealing prior to attempted rod movement).

Theoretical Common-Mode Software Failure	Consequences	Identification and Bounding End State
RCMS fails to apply Refueling Equipment Interlock during refueling operations.	No direct consequence to operation; Refueling Interlocks are designed as a back-up to reinforce unit administrative operating procedures and controls regarding in-vessel fuel movement.	Failure would be identified by weekly Channel Functional Test (CFT) Technical Specification Surveillance Requirement (TS SR). Administrative operating procedures and controls would preclude inadvertent criticality during refueling.
RCMS fails to apply Refuel Position One-rod-Out Interlock during Refuel.	No direct consequence; Refuel Position One-rod-Out Interlock is designed as a back-up to reinforce unit administrative operating procedures and controls regarding control rod withdrawal in Refuel.	Failure identified by neutron monitoring system and weekly CFT TS SR. Administrative operating procedures and controls would preclude inadvertent criticality during refueling.
RCMS fails to apply a control rod withdrawal block when required by safety related Rod Block Monitor (RBM) system instrumentation.	No direct consequence as RBM system is only applicable to High Power Control Rod Withdrawal Error (CRWE) event. EGC has verified that, in the event of an uncontrolled rod gang withdrawal event at power due to a common-mode software failure, the potential consequences will be bounded by the consequences of a previously analyzed accident.	Failure identified by neutron monitoring system and weekly CFT TS SR. Worst case end state is bounded by the consequences of a previously analyzed accident (i.e., the analytical consequences of a Control Rod Drop Accident (CRDA), LSCS Updated Final Safety Analysis Report (UFSAR) section 15.4.9.3 and UFSAR Table 15.4-6). End state evaluation described in response to NRC RAI SRXB-5 in Reference 3.

Theoretical Common-Mode Software Failure	Consequences	Identification and Bounding End State
RCMS fails to apply a control rod withdrawal block when required by Rod Worth Minimizer (RWM).	No direct consequence as RWM function is designed as a back-up to reinforce unit administrative operating procedures and controls regarding control rod withdrawal during low power operation. EGC has verified that, in the event of an uncontrolled rod gang withdrawal event at low power due to a common-mode software failure, the potential consequences will be bounded by the consequences of a previously analyzed accident.	Failure would be identified during CFT TS SR upon startup or shutdown when within required power level. Worst case end state is bounded by the consequences of a previously analyzed accident (i.e., the CRDA). End state evaluation is described in response to Reference 4, Attachment 2.
RCMS fails to apply a control rod withdrawal block when required by Reactor Mode Switch – Shutdown Position circuit.	No direct consequence as Reactor Mode Switch – Shutdown Position Rod Block is designed as a back-up to reinforce unit administrative operating procedures and controls prohibiting control rod withdrawal when in Shutdown.	Failure identified during CFT TS SR upon entering Shutdown. No resulting inadvertent criticality while Shutdown.
RCMS fails to apply a control rod withdrawal block when required by APRMs during normal power ascension.	Alarm followed by reactor scram from APRM High Set Point	Failure identified during CFT TS SR. No fuel damage occurs.
RCMS fails to apply a control rod withdrawal block when required by SRMs during normal power ascension or refueling operations.	Alarm followed by reactor scram from IRM High Set Point	Failure identified during CFT TS SR. No fuel damage occurs.

Theoretical Common-Mode Software Failure	Consequences	Identification and Bounding End State
RCMS fails to apply a control rod withdrawal block during power ascension or refueling operations when required by IRMs.	Alarm followed by reactor scram from IRM High Set Point	Failure identified during CFT TS SR. No fuel damage occurs.
RCMS fails to apply a control rod withdrawal block during power ascension or refueling operations when required by Scram Discharge Volume Water Level High Rod Block Instrumentation.	Reactor Scram from Scram Discharge Volume Water Level High Scram Set Point.	Failure identified during CFT TS SR. No fuel damage occurs.
RCMS fails to apply a control rod withdrawal block during power changes when required by Reactor Recirculation Pumps Flow Units.	Reactor Scram from APRM High Fixed Set Point.	Failure identified during CFT TS SR. No fuel damage occurs.
Loss of less than nine control rod RPIS Indications	TS Required Control Rod Insertion	Operating procedures ensure no thermal limit violation and hence no fuel damage
Loss of nine or more Control Rod RPIS Indications	TS Required Reactor Shutdown	All rods inserted and verified Full-in by direct PIP reading OR if time does not allow, a reactor scram will be inserted. If scram occurs or is necessary to meet TS, then until all control rods can be individually verified Full-in by direct PIP reading, ATWS Procedure will be followed to ensure reactor is shutdown and maintain decay heat removal. Analyzed ATWS consequences not exceeded.
Loss of Rod Drive Capability	TS required shutdown via manual scram required if repairs cannot be accomplished.	Reactor Shutdown by RPS with no adverse consequences.

Theoretical Common-Mode Software Failure	Consequences	Identification and Bounding End State
Loss of required Control Rod RPIS Indications combined with Loss of Rod Drive Capability	TS required shutdown via manual scram required if repairs cannot be accomplished.	After scram, until all control rods can be individually verified Full In by direct PIP reading, ATWS Procedure will be followed to ensure reactor is shutdown and maintain decay heat removal. Analyzed ATWS consequences will not be exceeded.
Unidentified loss of low pressure alarm function for HCU Accumulator Nitrogen Pressure.	No direct consequences as any actual low pressure accumulators would be found and recharged within TS SR weekly frequency for local accumulator pressure indication checks.	In the event that any portion of the control rods fail to fully insert on a scram due to unidentified inoperable accumulator, ATWS procedure will be followed to ensure reactor shutdown is accomplished and maintain decay heat removal. Analyzed ATWS consequences will not be exceeded.
Spurious single or gang rod withdrawal error at low or high power	Event terminated by single or gang of control rods reaching full out position unless preceded by an RPS auto scram from IRM or APRM High.	Analysis completed to show that the consequences are bounded by the results of the analyzed CRDA, as described in Attachment 2 of Reference 4 and in the response to SRXB-1 through SRXB-5 of Reference 3.